II. General Remarks Concerning This Response

Claims 1-25 are currently pending in the present application. The previous Office action contained an objection to dependent claims 2-5 (otherwise allowable) and indicated that claims 10-25 were allowable. In the present Office action, claims 1-4, 6-9, and 20-25 are now rejected. Claim 5 is objected as being dependent on a rejected claim but would be allowable if rewritten in independent form. Claims 10-19 have remained allowable. In response, claim 20 has been amended in this response; no claims have been added or canceled. Reconsideration of the claims is requested.

The previous rejection under 35 U.S.C. § 112 has been withdrawn in view of Applicant's arguments.

The previous rejection under 35 U.S.C. § 101 has been rewritten with a complete argument as compared to the previous Office action. In response, Applicant has amended independent claim 20 as suggested by the examiner to include a computer readable medium so that the system claim cannot be interpreted as claiming a mere computer program. The word "secret" has also been included in claim 20 as suggested to complete a phrase.

In a telephone interview with Examiner Moorthy on October 9, 2003, Applicant noted that the current Office action does not include a rejection of independent claim 1, although the Office action does state with respect to dependent claim 2 that is rejected over Vu in view of Raivisto "as applied to claim 1 above, and further in view of ...". Applicant confirmed with the examiner that the examiner erred in not including the rejection of claim 1 from the previous Office action into the current Office action, and it was the examiner's intention that the previous rejection of claim 1 was to have remained unchanged.

Therefore, with respect to prior art rejections in the present Office action, the obviousness rejection of independent claim 1 as being unpatentable over Vu in view of Raivisto has been continued from the previous Office action. In addition, a new obviousness rejection has been applied against dependent claim 2 over Vu and Raivisto and further in view of Gabber et al., and a new obviousness rejection has also been applied against independent claim 20 along with its dependent claims 21-24 and independent claim 25 over Hu and Raivisto. In response, Applicant has expanded the argument against the rejection of claim 2 and argues against the new rejections hereinbelow.

Applicant notes that the statement of the grounds of rejection for dependent claim 2 errs by not stating that the same grounds of rejection are applicable against dependent claims 3 and 4. Given the context of the Office action, though, it is apparent that the same grounds of rejection that are applicable for dependent claim 2 were also meant to be applied to claims 3 and 4.

However, the arguments for correcting the errors in the current Office action with respect to independent claim 1 and dependent claims 3 and 4 cannot be said to be true for dependent claims 6-9. The current Office action does not make any statement of the grounds of rejection for dependent claims 6-9, let alone actually present a rejection against claims 6-9. Although the current Office action discusses the previous rejection of claims 6-9 in the remarks section of the current Office action, the current Office action does not make any statement that reasonably implies that the rejections from the previous Office action were meant to be carried over from the previous Office action into the current Office action.

III. Summary of Present Invention

A method of enabling a proxy to participate in a secure communication between a client and a server. The method begins by establishing a first secure session between the client and the proxy. Upon verifying the first secure session, the method continues by establishing a second secure session between the client and the proxy. In the second secure session, the client requests the proxy to act as a conduit to the server. Thereafter, the client and the server negotiate a session master secret. Using the first secure session, this session master secret is then provided by the client to the proxy to enable the proxy to participate in secure communications between the client and the server. After receiving the session master secret, the proxy generates cryptographic information that enables it to provide a given service (e.g., transcoding, monitoring, encryption/decryption, caching, or the like) on the client's behalf and without the server's knowledge or participation. The first secure session is maintained between the client and the proxy during such communications.

IV. Comments on Examiner's Remarks About Previous Response

The examiner states the following on page 4, first paragraph: "The examiner asserts that the authentication process for the client's authorization to the requested services would have been the first session and communication process 19 would have been the second communication session." Applicant fails to understand how the examiner can continue to rely on Vu as teaching the claim elements when communication process 19 in Vu is clearly between the gateway/proxy 14 and the host server 46, whereas both communication sessions in the

claim elements are clearly stated as being between the client and the proxy.

The examiner then states the following on page 4, second paragraph:

> On page 26, the applicant argues that the combination of Vu and Raivisto does not show two communication sessions between a terminal/client and a mediator/gateway/proxy as claimed in the present invention. Examiner respectfully disagrees. As discussed above, Vu clearly teaches the claimed communication sessions. Vu was used to teach the client and the server negotiating a session master secret and delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication. Vu was not used to teach the two communication sessions between a terminal/client and a mediator/gateway/proxy.

The preceding paragraph is incomprehensible. Within the same paragraph, the examiner states that "Vu teaches the claimed communication sessions" while contradicting the first statement by stating that "Vu was not used to teach the two communication sessions". Moreover, the examiner states that "Vu was used to teach the client and the server negotiating a session master secret ..." when the original rejection contradicts this statement by stating that "Vu does not disclose having the client and the server negotiate a session master secret ..." on page 4 of the previous Office action.

V. 35 U.S.C. § 101—Double Patenting

The Office action has rejected claims 1, 6-10, 17, 18, and 20-25 of the present patent application in a statutory-type double patenting rejection over claims 1, 6-10, 17, 18, and 20-25 of Bellwood et al., U.S. Patent Number 6,584,567 B1, issued 06/24/2003, which is also assigned to IBM and has a common co-inventor with the present application. As

an initial issue, Applicant notes that the citation of the same claim numbers in the patent cannot be correct. In any case, this rejection is respectfully traversed.

MPEP § 804 states the following:

> A reliable test for double patenting under 35 U.S.C. 101 is whether a claim in the application could be literally infringed without literally infringing a corresponding claim in the patent. *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970). Is there an embodiment of the invention that falls within the scope of one claim, but not the other? If there is such an embodiment, then identical subject matter is not defined by both claims and statutory double patenting would not exist. For example, the invention defined by a claim reciting a compound having a "halogen" substituent is not identical to or substantively the same as a claim reciting the same compound except having a "chlorine" substituent in place of the halogen because "halogen" is broader than "chlorine".

The claims in the present patent application and the issued patent differ from each other. Independent claim 1 of the present application reads:

> 1. A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:
> establishing a first secure session between the client and the proxy;
> upon verifying the first secure session, establishing a second secure session between the client and the proxy, the second secure session requesting the proxy to act as a conduit to the server;
> having the client and the server negotiate a session master secret; and
> delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

Independent claim 1 of the issued patent reads as follows (emphasis has been added to show most of the differences between the two claims, particularly the additional subject material in the claim of the issued patent):

1. A method of enabling a proxy to participate in a secure communication between a client and a **first origin** server, comprising the step of:

(a) establishing a first secure session between the client and the proxy;

(b) upon verifying the first secure session, establishing a second secure session between the client and the proxy, the second secure session requesting the proxy to act as a conduit to the **first origin** server;

(c) having the client and the **first origin** server negotiate a session master secret;

(d) having the client deliver the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication;

(e) responsive to a client request to the first origin server, repeating steps (a)-(b) to enable the proxy to act as a conduit to a second origin server;

(f) having the client and the second origin server negotiate a new session master secret; and

(g) having the client deliver the new session master secret to the proxy using the first secure session generated in step (e).

As is apparent by a comparison of the claims in the present application and the issued patent, all of the independent claims in the issued patent contain additional subject matter concerning the use of the proxy between the client and multiple servers; this additional feature is not present in any of the independent claims nor dependent claims of the present application. Since the claims in the present patent application and the issued patent differ from each other, the claims cannot be considered to be drawn to the same invention for double patenting purposes under 35 U.S.C. § 101. Applicant requests the withdrawal of the double patenting rejection.

VI. 35 U.S.C. § 103(a)—Obviousness—*Vu* in view of *Raivisto*

The Office action has rejected claim 1 under 35 U.S.C. § 103(a) as unpatentable over Vu, "Apparatus and method for

providing a secure gateway for communication and data exchanges between networks", U.S. Patent No. 5,623,601, filed 11/21/1994, issued 04/22/1997, in view of Raivisto, "Method of implementing connection security in a wireless network", U.S. Patent Number 6,081,601, filed 01/27/1998, issued 06/27/2000. This rejection is respectfully traversed.

The beginning of the rejection of independent claim 1 states:

> As per claim 1, Vu discloses establishing a first secure connection between the client and the proxy (gateway station 14). Vu discloses that upon verifying the first secure session, establishing a second secure session between the client and the proxy (gateway station 14), the second secure session requesting the proxy to act as a conduit to the server, column 8 lines 54-64. Vu does not disclose having the client and the server negotiate a session master secret and delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

Vu clearly does not disclose some of the claimed features of the present invention, notwithstanding the arguments presented by the rejection. The portion of Vu that is cited by the rejection, column 8, lines 54-64, reads as follows:

> As will be explained below in detail, the process then authenticates the client's authorization to access the requested service and if the client 16 is determined to have the required authorization, the gateway station 14 initiates a second communication process 19 with the remote host 46 in which the gateway station 14 simulates the client 16 without revealing the client address. Once the two communication sessions 17, 19 are operative, communication is effected between the client 16 and the host 46 by passing communication data between the two interdependent communication sessions.

According to the rejection, the gateway in Vu is analogous to the proxy in the present application. The rejection states that Vu discloses at col. 8, lines 54-64,

that there are two communication sessions between the client and the gateway, but Vu does not disclose this. Vu discloses two communication sessions: one between the host server and the gateway and the other session between the gateway and the client. The cited portion of Vu refers to FIG. 4, which clearly shows a communication session (element 17) between the client (16) and the gateway/proxy (14) and a communication session (19) between the gateway/proxy (14) and external entities which route the data to the host (46).

Thus, in Vu, the gateway acts as an intermediary between the host and the client, and the client and the gateway communicate only through one communication session, whereas in the present invention, the client and the proxy communicate through two communication sessions. Independent claim 1 reads in its entirety:

> 1. A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:
> establishing a first secure session between the client and the proxy;
> upon verifying the first secure session, establishing a second secure session between the client and the proxy, the second secure session requesting the proxy to act as a conduit to the server;
> having the client and the server negotiate a session master secret; and
> delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

In the present application, after establishing a first communication session between the client and the proxy, the client then establishes a second communication session between the client and the proxy. The second communication session is established through the proxy such that the proxy acts as a conduit or tunnel. For this second communication session, the proxy merely transfers the content between the client and the

server, and the proxy does not actively process the content, such as transcoding the content or some other function. After the client obtains a session master secret from the server through the second communication session, the client transfers the session master secret to the proxy using the first communication session, after which the client communicates with the server through the first communication session. The proxy and the client maintain the first secure session, and the server is unaware that it is communicating with the proxy using the session master secret rather than the client; in a typical, prior art case, the server would communicate directly with the client using the session master secret. With the present invention, the proxy performs its active processing, such as transcoding content, with the message traffic through the first communication session. In addition, the entire communication channel remains secure with the server unaware that the proxy is acting as an intermediary between the client and the server.

Hence, the rejection of claim 1 contains a fundamental flaw in that it argues that Vu discloses two communications sessions between the proxy (gateway station in Vu) and the client, but this is incorrect. The rejection then proceeds to rely on Raivisto to remedy another deficiency in Vu with respect to the secure characteristic of the communication sessions in claim 1. However, Raivisto clearly discloses a similar arrangement of communication elements.

The rejection combines the teachings of Vu and Raivisto by stating: "A first secure connection will be made between a client (MS1) and a proxy (MD). A second connection will be made between a client (MS1) and a proxy (MD) that enables the proxy to act as a conduit to the server. Secret keys will be established [sic] the proxy (MD) and the client (MS1) and the

proxy (MD) and the server (MS2)." This combination apparently argues that an analogy can be made between the proxy of the present invention and the mediator of Raivisto, but it does not explain how the prior art shows two communication sessions between a terminal/client and a mediator/gateway/proxy as claimed in the present invention.

In other words, the combination of Raivisto with Vu does not remedy the most prominent deficiency in Vu because the basic configuration of Raivisto is similar to Vu. In Raivisto, the mediator acts as an intermediary between two terminals; this configuration is analogous to the gateway acting as an intermediary between the host and the client in Vu or the proxy acting as an intermediary between the server and the client in the present invention. However, Raivisto does not disclose two communication sessions between a single terminal and the mediator, as would be necessary before Raivisto can begin to disclose the claimed features of the present invention concerning two secure communication sessions between a client and a proxy.

Examiner bears the burden of establishing a *prima facie* case of obviousness.

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Only when a *prima facie* case of obviousness is established does the burden shift to the applicant to produce evidence of nonobviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). If the Patent Office

does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to the grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). In response to an assertion of obviousness by the Patent Office, the applicant may attack the Patent Office's *prima facie* determination as improperly made out, present objective evidence tending to support a conclusion of nonobviousness, or both. *In re Fritch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992).

With respect to claim 1, Vu in view of Raivisto does not disclose the claimed invention nor provide any suggestion to motivate one having ordinary skill in the art to modify the prior art to reach the claimed invention. In fact, the rejection appears to disregard entire claim elements without justification. In general, the rejection does not point out the necessary teachings, suggestions, or incentives to reach the claimed invention. Hence, the rejection of claim 1 does not establish a *prima facie* case of obviousness based on the prior art. Therefore, the rejection of claim 1 under 35 U.S.C. § 103(a) has been shown to be insupportable, and this claim is patentable over the applied prior art. Applicant requests the withdrawal of the rejection.

VI. 35 U.S.C. § 103(a)—Obviousness—*Vu* in view of *Raivisto* and further in view of *Gabber et al.*

The Office action has rejected claim 2 (and supposedly also claims 3 and 4) under 35 U.S.C. § 103(a) as unpatentable over Vu in view of Raivisto and further in view of Gabber et al., "System and method for providing anonymous personalized browsing by a proxy system in a network", U.S. Patent Number

5,961,593, filed 01/22/1997, issued 10/05/1999. This rejection is respectfully traversed.

The rejection of dependent claim 2 states that "Gabber et al. teaches a proxy that uses a session master secret and a session identifier to generate cryptographic information [column 7, lines 40-54]". The rejection confusingly contains two motivational statements. The first motivational statement merely restates the claimed feature in claim 2, and it is unclear why the first motivational statement is included. The second motivational statement states that it would have been obvious to include the teaching of Gabber et al. into a hypothetical combination of the teachings of Vu and Raivisto "because there is no permanent secret information stored on the proxy system [column 7, lines 43-46]". Applicant fails to understand how the fact that the system of Gabber et al. does not store secret information on a proxy would have motivated one of ordinary skill to use the recited feature to generate cryptographic information in a hypothetical system that combines the teachings of Vu and Raivisto. The ability to generate cryptographic information at the proxy is independent and distinct issue with respect to the design decision not to store secret information at the proxy. In other words, there is no nexus between the cited feature and the provided motivation. Moreover, the inclusion of features from Gabber et al. would have resulted in a change in the principle of operation of the system that is disclosed in Vu or Raivisto or a hypothetical combination of both. For these and other reasons, Applicant asserts that one would not have been motivated to combine teachings from Gabber et al. into a hypothetical system that combines the teachings of Vu and Raivisto.

With respect to dependent claims 3 and 4, these claims recite the features that a proxy modifies requests and responses from/to a client and performs a service on behalf of a client. Given that dependent claims 3 and 4 are dependent upon claim 2, claims 3 and 4 are non-obvious over a combination of Vu, Raivisto, and Gabber et al. for the same reasons as claim 2. Since the rejection of claims 2-4 does not establish a *prima facie* case of obviousness based on the prior art, the rejection of claims 2-4 under 35 U.S.C. § 103(a) is insupportable, and these claims are patentable over the applied prior art. Applicant requests the withdrawal of the rejection.

VII. 35 U.S.C. § 103(a)—Obviousness—*Hu in view of Raivisto*

The Office action has rejected claims 20-25 under 35 U.S.C. § 103(a) as unpatentable over Hu, "Method and apparatus for authenticating a client to a server in computer systems which support different security mechanisms", U.S. Patent No. 5,586,260, filed 02/12/1993, issued 12/17/1996, in view of Raivisto, "Method of implementing connection security in a wireless network", U.S. Patent Number 6,081,601, filed 01/27/1998, issued 06/27/2000. This rejection is respectfully traversed.

A portion of the rejection of independent claim 20 states:

> Hu does not teach controlling the client to negotiate with the server through the conduit to obtain a session master secret. Hu does not teach controlling the client to deliver the session master secret to the proxy using the first secure session. Hu does not teach a computer program for controlling the proxy to use the session master secret and a session identifier to generate given cryptographic information. Hu does not teach that the proxy modifies content in communications between the client and the server.

The rejection cites most of column 4 of Hu in support of an argument that Hu discloses some of the claimed features. However, the portion of Hu at column 4, lines 59-66, that is cited in support of the rejection's assertion that Hu discloses "controlling the client to request a second secure connection to the proxy" does not disclose this feature; this portion of Hu reads as follows:

> A server typically has as part of its security mechanism the means to check an access control list (ACL) to determine whether a client seeking access has been duly authorized. The ACL contains an entry for each "principal" identity, and principals are identified by a certificate issued by some trusted authority, such as a security server. To obtain the certificate, a principal must first log in using either a secret key or a password.

While the cited portion of Hu discusses certificates, the cited portion of Hu clearly does not support the claimed feature as asserted by the rejection. More importantly, though, the rejection asserts that Hu teaches two simultaneous sessions between the client and the gateway/proxy. This is incorrect. In the system disclosed in Hu, the client uses a first communication session with the gateway, which logs into the server on behalf of the client to obtain credentials and then caches the credentials; the first session is then concluded. During a second communication session at a later time, the client calls the gateway/proxy to send a request to the server, and the gateway/proxy obtains the cached credentials and calls the server on behalf of the client. Thus, the two communication sessions between the client and the gateway/proxy are not simultaneous. Hence, the rejection of claim 20 contains a fundamental flaw in that it argues that Hu discloses two communications sessions between the gateway/proxy and the client, but this is incorrect.

As admitted in the rejection, Hu clearly does not disclose many of the claimed features of the present invention. The rejection then proceeds to rely on Raivisto as disclosing certain claimed features with respect to the secure characteristic of the communication sessions. Assuming, *arguendo*, that Raivisto discloses the claimed features as asserted, it would not have been possible to modify the system that is disclosed in Hu to incorporate the features of Raivisto without major modifications to the system of Hu that completely changed the principle of operation of the system of Hu. In the system of Hu, the gateway/proxy cannot act in the capacity as a conduit between the client and the server; the client calls the gateway/proxy to initiate the authentication process to the server, and the client calls the gateway/proxy to initiate the sending of requests from the gateway/proxy to the server. The client is not able to generate requests to the server that are merely passed through the gateway/proxy to the server, and in the other direction, responses from the server cannot be merely passed back through the gateway/proxy to the client. In the system of Hu, all security-related information is cached and controlled by the gateway/proxy. Hu specifically teaches that the gateway/proxy must operate in this manner at multiple places. For example, the abstract of Hu states: "A method and corresponding apparatus for authenticating a client for a server when the client and server have different security mechanisms." As another example, Hu states at column 3, lines 59-62: "A client system, indicated by reference numeral 10, wishes to use the services provided by a server system 12, but does not have the required software or hardware to conform to the server's requirements for authentication."

Hence, Applicant asserts that Hu actually teaches away from the present invention because Hu specifically states that the client is not able to conform to the server's requirements for authentication. It would not be possible for the system of Hu to control "the client to negotiate with the server through the conduit to obtain a session master secret" as is required by the claim language in the present application. Hence, the motivational statement that is provided in the rejection, which states that "the client and the server would have negotiated a master secret", contradicts the abilities of the system that is disclosed in Hu. If the system of Hu were modified to include the claimed features as argued by the motivational statement, then the advantages of the system of Hu would be negated; the client would be required to be modified to include security mechanisms that correspond with the capabilities of the server, which was avoided by the solution of Hu. More importantly, if the client could negotiate a master secret with the server, then most of the functionality of the gateway/proxy in the system of Hu would be unnecessary, which is contrary to what is taught by Hu.

Independent claim 25 was rejected with the same arguments as independent claim 20. Thus, the arguments that were provided above with respect to the patentability of claim 20 are applicable to claim 25. Dependent claims 21-24 were rejected as having features that are inherent to a proxy. Applicant asserts that these features are not necessarily inherent in a proxy, and Applicant asserts that the rejection improperly uses an inherency argument. More importantly, the arguments that were provided above with respect to the patentability of claim 20 are applicable to claims 21-24 based on their dependency on claim 20.

With respect to claims 20-25, Hu in view of Raivisto does not disclose the claimed invention nor provide any suggestion to motivate one having ordinary skill in the art to modify the prior art to reach the claimed invention. In general, the rejection does not point out the necessary teachings, suggestions, or incentives to reach the claimed invention. In fact, the rejection appears to disregard entire claim elements without justification, and the rejection argues for the inclusion of features from a secondary reference into a primary reference that would fundamentally alter the operation of the system that is disclosed in the primary reference. Hence, the rejection of the claims does not establish a *prima facie* case of obviousness based on the prior art. Therefore, the rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable, and these claims are patentable over the applied prior art. Applicant requests the withdrawal of the rejection.

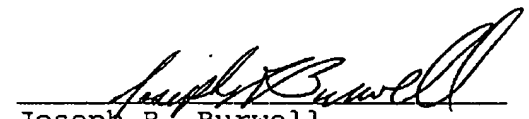
VIII. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: November 17, 2003

Respectfully submitted,



Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755-8022
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz